Chiragowni Rahul Goud* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.6, Issue No.5, August - September 2018, 8594-8596.

A Rigid Dual Phase Control Approach for Online Cloud Computing Services

CHIRAGOWNI RAHUL GOUD
M.Tech Student, Dept of CSE, Nagole Institute of Technology and Science, Hyderabad, T.S, India

S.SREE HARI RAJU
Assistant Professor& HOD, Dept of CSE, Nagole Institute of Technology and Science, Hyderabad, T.S, India

Abstract: **We offer a completely new access control system (2-FA) and two-factor authentication for cloud-based cloud services. Specifically, under the access control system we use from two FA modules, access control features are implemented with a person's secret key and a lightweight security device. Because the user cannot connect somewhere when they do not have a connection, the machine can improve peace of mind on the device, especially in individual scenarios where many users share the exact same computer for cloud-based services. There are two issues with your account / password system. First, traditional account / password-based authentication is not based on maintaining privacy. Under the signature or understanding formula, take the main factor along with the SEM together. In addition, object-based control within the system also allows the cloud server to restrict the use of individual users with the same number of features while maintaining user privacy, meaning that the cloud server understands only that the client complies with the correct document, but does not work. The minute inside the user. Under Validate Signature or Encryption Format, the client's public key takes the corresponding identity. Finally, we implemented a simulation to demonstrate practical capability within our proposed dual system.**

Keywords: **Fine-Grained; Two-Factor; Access Control; Web Services;**

I. INTRODUCTION:

The first to be signed before the use of cloud services or have the ability to view the confidential data stored within the cloud required. There are two issues with your account / password system. First, the account / password is not traditional authentication based on maintaining privacy. The proposed new access control model, known as access control based on characteristics, is a good candidate to deal with the first problem. Not only does it provide anonymous authentication, but also determines access control policies according to the characteristics of the applicant, the atmosphere or perhaps the information object. There are many applications of cloud computing, for example, data discussion, data storage, huge data management, medical information system, etc [1]. The benefits of cloud services and cloud computing are enormous based, simplicity as simplicity, reduce costs and capital expenditure, high operational efficiency, Flexibility and time to yourself in the market. In access-based access control system, 1 includes each user this type of user secret power. Having thought about the above problem in web services, it is common that computers are shared by many users, especially in large organizations or organizations. Two-FA is very common among online banking. In addition to having a user name / password, the client may also need a device to test the password once. Some systems may require the customer to obtain a cell phone to be sent a one-time password to the cell phone via SMS during the login process. Using two FFA, users can gain more confidence in using common computers to sign in to online banking online. For the same reason, it would be better for FA-FA-2 users within the cloud services to improve the security of the system [2]. In this document, we recommend using dual-access control protocol as the key factors to calculate cloud services on the Internet, with security and light weight. With this device, our security protocol provides FA-DOS. Our protocol support provides access based on the excellent versatility of the system to create different policies based on different access scenarios. At the same time, it can also maintain privacy within the user. The cloud system only includes the client offering some of the required tasks, while no specific identity within the user. First there is a need for client confidentiality. Only customers can grant access when all products are available. Additionally, the client cannot use your secret key with another device for others to access.

II. PREVIOUS DESIGN:

Although the new cloud computing model offers benefits, you will also find privacy and security concerns specifically for web-based cloud services. Because confidential data can be kept in the cloud to analyze the purpose or convenient access, and qualified users can also communicate with the system in the cloud to obtain a series of services and applications, user authentication has become a central component of any system in the cloud. It requires a person to log in before using cloud services or accessing confidential data in the cloud. There are two problems with the account / password system. Disadvantages of the current system: First, the standard authentication account /

password is not maintaining privacy. However, it is recognized that privacy is a vital feature that should be considered in cloud computing systems. Second, it is common to talk about a computer among different people. It can be easy for hackers over the Internet to configure some spyware tools to understand the login password in a web browser [3]. In the current situation, although the computer may be locked with a password, it may be possible to suspect it or steal it through unwritten software.

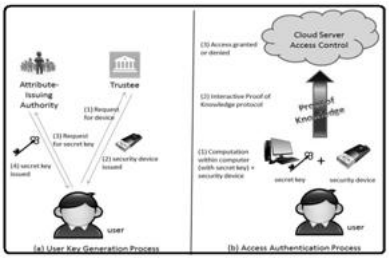

Fig.1.Proposed scheme

III. ENHANCED CONTROL:

We recommend the two-factor access control protocol for cloud-based cloud services, which uses a lightweight security device. The unit has the following characteristics: (1) It can calculate some lightweight algorithms, for example. Retail and resistance to manipulation, that is, it is assumed that no one can access it to obtain confidential information stored inside. Benefits of the proposed system: Our protocol provides 2FA security. Our protocol supports access based on specific attributes that provide excellent system versatility to create different access policies based on different scenarios. At the same time, you can also maintain user privacy. In addition, it can generate random numbers and an exponentiations account in the specified periodic group instead of a limited field [4]. The unit configuration process includes a two-tiered sword. The Setupstarts by getting an administrator to create generic parameters. The second part of ASetup works using the power-issuing features to create the key secret key and public key. The process of creating the client key involves three parts. First, the client creates its secret and public type in the USetup. Your home alarm system is configured using the administrator to configure the devices. Finally, the attribute-issuing authority creates the client's confidential attribute type online using the AttrGen user attribute. Access authentication is an interactive protocol that is associated with the user as well as the cloud company. Effortlessly, a few parts protocol may be a system of understanding testing if one party believes that the other really knows some "knowledge". To demonstrate that our creation of PK1 is a zero understanding of the authentic verification checker, we simply demonstrate the creation of another S emulator, which is able to transmit the text in each PK1 in the input challenge c. Do you assume that the original claim is more? It is determined by using the attacker. It refers to a discount that violates authentication security, and access without a security device or access without a secret key, whether it can be effectively documented for the document. We measure the efficiency of our protocol in 50% of the pieces. In part, we know the main processes of the authentication protocol [5]. The basic concept of encryption is to use an online moderator for each transaction. This online broker is known as SEM because it provides a cost for security skills. When SEM does not cooperate, it is no longer possible to perform transactions while using the public key. In an SMC system, a person has a secret key and a public key along with an identity. Under the signature or understanding formula, take the underlying factor together with SEM. Under the signature or encryption verification format, take the customer's public key with the corresponding identity. Because SEM is controlled by a specialist typically used to process user revocation, the authority will not provide any collaboration to any disabled user. Therefore, revoked users cannot create signatures or decrypt encrypted text. The main reason behind SMC should be to solve the problem of revocation. Thus, SMEs are controlled using power. Basically, you must be online authority for each signature and understand the encrypted text. The client is not anonymous in the SMC. During physics, the security method is controlled by the user. The anonymity can also be maintained. The general concept of safety with the main isolation ended up storing long-term keys inside a physical security device but limited in calculation. The important thing in the process of updating the agent requires a protection device. When the key remains up to date, the signature or understanding version will not need the system within the same time period. Although our concept requires a security device every time the client tries to interact with the device. Short-term password keys are stored by users around the effective but unsafe device where encryption accounts occur. Temporary secrets are likely to be updated at separate intervals through the user-related interaction with the rule, as the public key remains unchanged with the device's time period [6].

IV. CONCLUSION:

During this document, we present a completely new approach to controlling access via the Internet (FA) for cloud-based cloud services. Through the performance evaluation, we showed that the event "was worth it". Within the signature or comprehension formula, take the main factor along with the SEM together. Under the signature verification or encryption format, the customer's

public key takes the corresponding identity. The detailed security analysis ensures that the proposed access control system (FA) for two units (FA) can achieve highly desirable security requirements. By using the access control mechanism based on the attribute, the access control system proposed for the FA units remains specific not only to allow the server in the cloud to limit the use of committed individual users with the same number of functions, but also to maintain the user's privacy. We leave it as an attempt in the future to improve the efficiency and all kinds of highlights of the unit.

V. REFERENCES:

[1] F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, and P. Krause, "An efficientPHR service system supporting fuzzy keyword search and fine-grainedaccess control," Soft Compute., vol. 18, no. 9, pp. 1795–1802, 2014.

[2] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013.

[3] T. Okamoto and K. Takashima, "Efficient attribute-based signatures for non-monotone predicates in the standard model," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 6571. Berlin, Germany: Springer-Verlag, 2011, pp. 35–52.

[4] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Security-mediated certificate less cryptography," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp. 508–524.

[5] Y. Dodis and A. Yampolskiy, "A verifiable random function with short proofs and keys," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 416–431.

[6] X. Huang et al., "Cost-effective authentic and anonymous data sharing with forward security," IEEE Trans. Compute., vol. 64, no. 4, pp. 971–983, Apr. 2015.

